LAW OFFICES
SUGHRUE, MION, ZINN, MACPEAK & SEAS, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
WASHINGTON, DC 20037-3213
TELEPHONE (202) 293-7060
FACSIMILE (202) 293-7860
www.sughrue.com

October 5, 2000

BOX PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Re: Junichi KOKUDO
AUTHENTICATION METHOD AND APPARATUS
AT WIRELESS LAN SYSTEM
Our Ref. Q61120

Dear Sir:

Attached hereto is the application identified above including 19 sheets of the specification, claims, 6 sheets of formal drawings, executed Assignment and PTO 1595 form, and executed Declaration and Power of Attorney.

The Government filing fee is calculated as follows:

Total claims	11	- 20	=		x	$18.00	= $.00
Independent claims	2	- 3	=		x	$80.00	= $.00
Base Fee							$710.00
TOTAL FILING FEE							**$710.00**
Recordation of Assignment							$40.00
TOTAL FEE							**$750.00**

Checks for the statutory filing fee of $710.00 and Assignment recordation fee of $40.00 are attached. You are also directed and authorized to charge or credit any difference or overpayment to Deposit Account No. 19-4880. The Commissioner is hereby authorized to charge any fees under 37 C.F.R. §§ 1.16 and 1.17 and any petitions for extension of time under 37 C.F.R. § 1.136 which may be required during the entire pendency of the application to Deposit Account No. 19-4880. A duplicate copy of this transmittal letter is attached.

Priority is claimed from October 5, 1999 based on Japanese Application No. 284231/1999. The priority document is enclosed herewith.

Respectfully submitted,
SUGHRUE, MION, ZINN,
MACPEAK & SEAS, PLLC
Attorneys for Applicant

By: _____
J. Frank Osha
Registration No. 24,625

J. Kokudo
Filed 10/4/00
Q61120
1 of 1

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

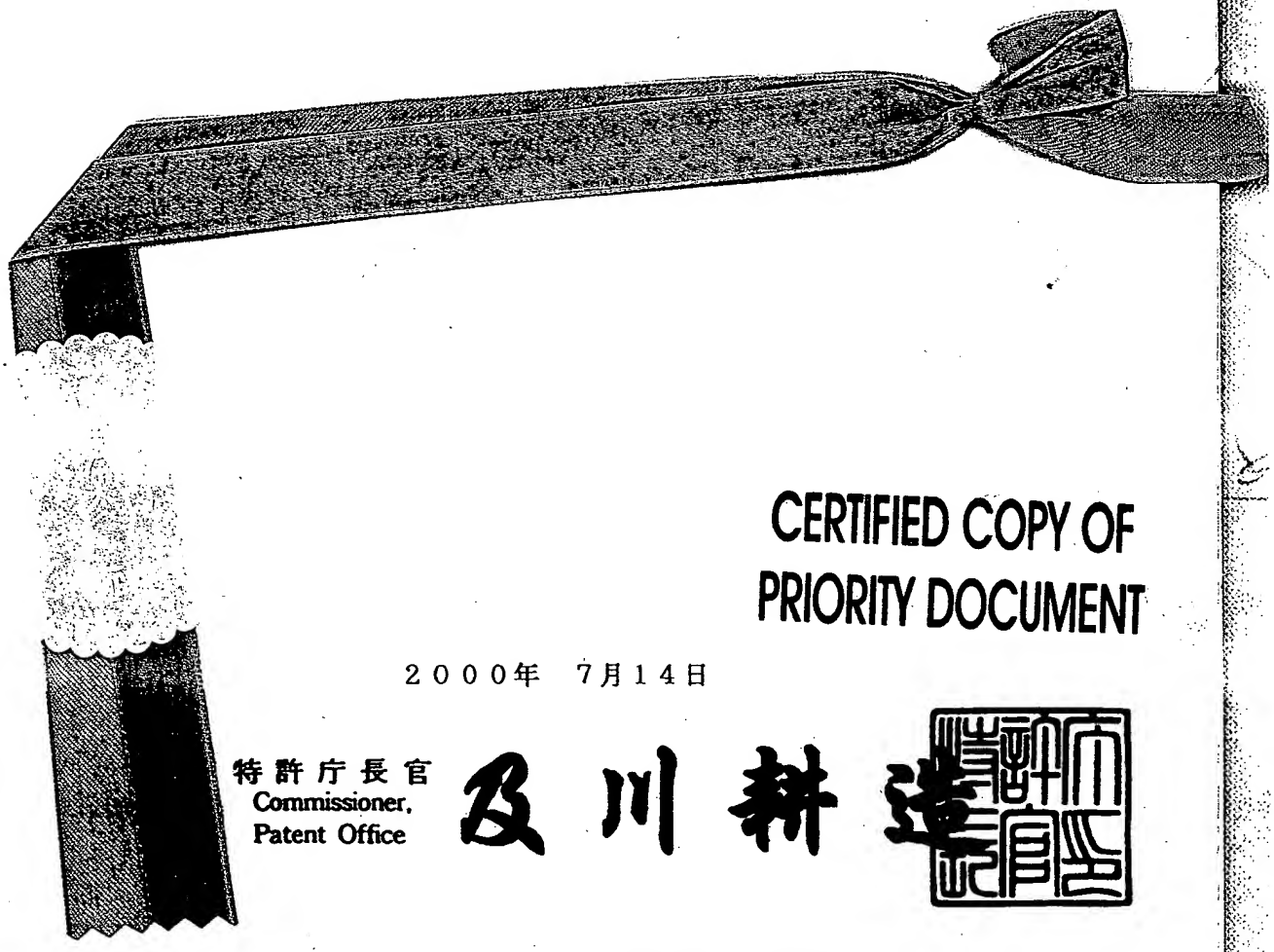
This is to certify that the annexed is a true copy of the following application as filed with this Office.

JC841 U.S. PTO
09/680258
10/05/00

出願年月日
Date of Application: １９９９年１０月　５日

出願番号
Application Number: 平成１１年特許願第２８４２３１号

出願人
Applicant (s): 日本電気株式会社



CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年　７月１４日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０５４４５６

【書類名】　特許願

【整理番号】　49230041

【あて先】　特許庁長官　殿

【国際特許分類】　H04L 12/28

H04B 7/26

H04Q 7/04

【発明者】

【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内

【氏名】　國土　順一

【特許出願人】

【識別番号】　000004237

【氏名又は名称】　日本電気株式会社

【代理人】

【識別番号】　100082935

【弁理士】

【氏名又は名称】　京本　直樹

【電話番号】　03-3454-1111

【選任した代理人】

【識別番号】　100082924

【弁理士】

【氏名又は名称】　福田　修一

【電話番号】　03-3454-1111

【選任した代理人】

【識別番号】　100085268

【弁理士】

【氏名又は名称】　河合　信明

【電話番号】　03-3454-1111

【手数料の表示】

【予納台帳番号】　008279

【納付金額】　　21,000円

【提出物件の目録】

【物件名】　　明細書　1

【物件名】　　図面　1

【物件名】　　要約書　1

【包括委任状番号】　9115699

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】無線ＬＡＮシステムにおける認証方法と認証装置

【特許請求の範囲】

【請求項１】　無線ＬＡＮシステムにおける認証方法において、

端末局（ＳＴＡ）は帰属しようとするアクセスポイント（ＡＰ）に対して認証要求し、

前記ＡＰは認証サーバに対して前記認証サーバに適合するプロトコルに変換して認証要求し、

前記認証サーバは前記ＳＴＡのＭＡＣアドレスに基づき認証し、

前記ＡＰは前記ＳＴＡと所定の暗号化アルゴリズムに基づき暗号化認証を行なうことを特徴とする無線ＬＡＮシステムにおける認証方法。

【請求項２】　前記暗号化認証が正常に完了した後、前記認証サーバからの指示により前記ＡＰのＭＡＣアドレスのテーブルを更新することを特徴とする請求項１記載の無線ＬＡＮシステムにおける認証方法。

【請求項３】　前記認証サーバに障害が発生した場合に、前記ＡＰ単独にて前記ＭＡＣアドレスの認証を行なうことを特徴とする請求項１記載の無線ＬＡＮシステムにおける認証方法。

【請求項４】　前記暗号化アルゴリズムは、予め定められた使用期限を有する共通鍵に基づき暗号化されていることを特徴とする請求項１記載の無線ＬＡＮシステムにおける認証方法。

【請求項５】　前記共通鍵の期限が切れた場合に、オープンシステム認証方式によりＭＡＣアドレス認証することを特徴とする請求項４記載の無線ＬＡＮシステムにおける認証方法。

【請求項６】　前記オープンシステム認証方式の場合は、アソシエーションした後、通信を行なう期間に所定の短時間の制限を設け、前記制限された時間内に鍵配送することを特徴とする請求項５記載の無線ＬＡＮシステムにおける認証方法。

【請求項７】　無線ＬＡＮシステムにおける認証装置において、

端末局（ＳＴＡ）と所定の暗号化アルゴリズムに基づき認証すると共に認証サ

ーバと接続し、認証に関わる信号を前記認証サーバに適合するプロトコルに変換するアクセスポイント（ＡＰ）と、

前記変換された認証要求を受けて前記ＳＴＡのＭＡＣアドレスに基づき認証する前記認証サーバと

を有することを特徴とする無線ＬＡＮシステムにおける認証装置。

【請求項８】　前記ＡＰは、前記暗号化認証が正常に完了した後、前記認証サーバからの指示により前記ＡＰのＭＡＣアドレスのテーブルを更新する手段を有することを特徴とする請求項７記載の無線ＬＡＮシステムにおける認証装置。

【請求項９】　前記ＡＰは、前記認証サーバが故障した場合に、単独で前記ＭＡＣアドレスの認証を行うことを特徴とする請求項７記載の無線ＬＡＮシステムにおける認証装置。

【請求項１０】　前記所定の暗号化アルゴリズムは、ＩＥＥＥ８０２．１１に規定されたＷＥＰアルゴリズムであることを特徴とする請求項７記載の無線ＬＡＮシステムにおける認証装置。

【請求項１１】　前記暗号化アルゴリズムは、使用期限を有する共通鍵を用いることを特徴とする請求項７記載の無線ＬＡＮシステムにおける認証装置。

【請求項１２】　前記共通鍵の期限が切れた場合に、オープンシステム認証方式によりＭＡＣアドレス認証することを特徴とする請求項１１記載の無線ＬＡＮシステムにおける認証装置。

【請求項１３】　前記オープンシステム認証方式の場合は、アソシエーション後に、通信を行なう時間に所定の短時間の制限を設け、前記制限された時間内に鍵を配送することを特徴とする請求項１２記載の無線ＬＡＮシステムにおける認証装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は無線ＬＡＮシステムの認証方法において、特にＩＥＥＥ８０２．１１（米国電気電子技術者協会で規定した国際標準）に準拠した無線ＬＡＮシステムの認証方法と認証装置に関する。

【０００２】

【従来の技術】

ＩＥＥＥ８０２．１１に準拠した無線ＬＡＮシステムは、今後普及が見込まれており免許不要で使用できる周波数帯（２．４ＧＨｚや５ＧＨｚ）を使用できることから、無線区間のセキュリティ確保が重要になっている。

【０００３】

ＩＥＥＥ８０２．１１の第８章認証と暗号（８．ＡＵＴＨＥＮＴＩＣＡＴＩＯＮ　ＡＮＤ　ＰＲＩＶＡＣＹ）には、オープンシステムを用いた認証方式（ＯＰＥＮ　ＳＹＳＴＥＭ　ＡＵＴＨＥＮＴＩＣＡＴＩＯＮ）とＷＥＰ（ＷＩＲＥＤ　ＥＱＵＩＶＡＬＥＮＴ　ＰＲＩＶＡＣＹ）アルゴリズムを用いた共通（秘密）鍵認証方式（ＳＨＡＲＥＤ　ＫＥＹ　ＡＵＴＨＥＮＴＩＣＡＴＩＯＮ）とが規定されており、認証方式としてオープンシステム認証方式と共通鍵認証方式の２種類のどちらかが固定的に使用される。

【０００４】

図５は、ＩＥＥＥ８０２．１１に規定された無線ＬＡＮシステムの暗号化認証に関わる部分のブロック図を示す。

【０００５】

本図において、ＳＴＡ(ＳＴＡＴＩＯＮ)１は、複数の端末局であり、各端末局は無線信号の送受信機能を有するノートＰＣ等のデータ端末である。

【０００６】

ＡＰ（アクセスポイント；ＡＣＣＥＳＳ　ＰＯＩＮＴ）２は、無線アクセスと有線網とのインターフェース機能や無線信号の送受信機能を有し、さらに無線信号制御等のファームウェアやＭＡＣアドレス認証機能も搭載されている。

【０００７】

保守サーバ４は、ＡＰ２をＳＮＭＰで設定、管理を行なうサーバである。

【０００８】

ＳＴＡ１とＡＰ２間の接続は無線区間５となっており、ＡＰ２と保守サーバ４間の接続はイーサーネット等の有線区間が用いられている。

【０００９】

最初に、共通鍵認証方式について図を用いて説明する。

【００１０】

図６は、ＩＥＥＥ８０２．１１で規定されたＷＥＰアルゴリズムを用いた暗号化認証手順を示したシーケンス図である。本図において、ＷＥＰアルゴリズムによる暗号化認証はＯＳＩ（ＯＰＥＮ　ＳＹＳＴＥＭ　ＩＮＴＥＲＣＯＮＮＥＣＴＩＯＮ）の第２層のデータリンク層の副層であるＭＡＣ（媒体アクセス制御；ＭＥＤＩＡ　ＡＣＣＥＳＳ　ＣＯＮＴＲＯＬ）において行われている。

【００１１】

なお、ＭＡＣは、複数の装置からのデータ送信要求が共通の伝送路上で競合したときのアクセス権制御や、装置と伝送路の物理的接続点の識別、フレーム形成、伝送路上の誤り制御などを第１層の物理層（ＰＨＹ；ＰＨＹＳＩＣＡＬ　ＬＡＹＥＲ）と一体化して行なう。

【００１２】

あるＳＴＡ１からＡＰ２に対して認証要求が無線信号にて送信される（Ｓ１）。このとき、ＰＤＵフォーマット内には共通鍵による認証要求であることを示すビットが用意されている。また、ＭＡＣフレーム内にはソースアドレスとしてＳＴＡ１のＭＡＣアドレスが含まれている。

【００１３】

認証要求を受けたＡＰ２からＳＴＡ１に対してチャレンジテキストが送出される（Ｓ２）。チャレンジテキストを受けたＳＴＡ１は、ＷＥＰアルゴリズムに基づいて自分の共通鍵とＩＶ（イニシャライゼイション　ベクター；ＩＮＩＴＩＡＬＩＺＡＴＩＯＮ　ＶＥＣＴＯＲ）により暗号化する（Ｓ３）。

【００１４】

次に、ＳＴＡ１は、暗号文とＩＶをＡＰ２に対して送信する（Ｓ４）。ＡＰ２は、受信した暗号文とＩＶと自分の共通鍵により暗号文を復号化し、Ｓ２で送信したチャレンジテキストとＳ４で得られたチャレンジテキストとを比較して一致／不一致を判定する（Ｓ５）。

【００１５】

ＡＰ２は、Ｓ４の判定結果が一致していた場合には、全体の認証が完了したと

して認証完了通知としてＳＵＣＣＥＳＳＦＵＬ　ＣＯＤＥをＳＴＡ１に送信する（Ｓ６）。認証完了通知を受けたＡＰ１はＳＴＡ２とアソシエーション（ＡＳＳＯＣＩＡＴＩＯＮ）の動作に移行する（Ｓ７）。

【００１６】

一方、オープンシステム認証方式は、ＳＴＡ１からＡＰ２に認証要求を送出すると、特段の確認手順を持たずに、ＡＰ２からＳＴＡ１に対して認証結果が送出されるという簡単な手順である。

【００１７】

【発明が解決しようとする課題】

以上説明したＩＥＥＥ８０２．１１の規定に準拠した無線ＬＡＮシステムにおける認証方法及び認証装置では、以下のような課題がある。

【００１８】

第１に、前述した無線ＬＡＮシステムではＡＰ２がＭＡＣアドレスを認証している。しかし、一般にＡＰ２は無線アクセスと有線アクセスとのインターフェース機能をメインタ
スクとしているため、ＭＡＣアドレス認証機能のためのハードウェアやソフトウェアには制限がある。特に、通常用いられるＡＰ２では、多数のＳＴＡ１（例えば、１０，０００台以上のＳＴＡ１）のＭＡＣアドレステーブルを用意するのは難しいため、多数のＳＴＡ１に対してＭＡＣアドレス認証をすることが困難であった。

【００１９】

第２に、最近は無線ＬＡＮシステムの端末局に無線信号を制御するためのファームウェアやＩＤ等が記憶されたカードが用いられるようになってきている。このような無線ＬＡＮシステムにＩＥＥＥ８０２．１１で規定された共通鍵認証方式を適用するためこのカードに鍵を記憶した場合には、カードは小型で持ち運び容易で、置き忘れや盗難し易く不正使用される確率が大きいため安全性を高める手段が必要となっていた。

【００２０】

第３の課題は、オープンシステム認証方式では認証処理を完了し、アソシエー

ション後の通信期間に制限が無かったので、不正接続される可能性があり安全性が低かった。

【００２１】

以上説明したように本発明の目的は、これらの問題を解決した無線ＬＡＮシステムの認証方法および認証装置を提供することにある。

【００２２】

【課題を解決するための手段】

本発明は上述した課題を解決するため、無線ＬＡＮシステムにおける認証方法において、端末局（ＳＴＡ）は帰属しようとするアクセスポイント（ＡＰ）に対して認証要求し、

前記ＡＰは認証サーバに対して前記認証サーバに適合するプロトコルに変換して認証要求し、前記認証サーバは前記ＳＴＡのＭＡＣアドレスに基づき認証し、前記ＡＰにチャレンジテキストを送出し、前記ＡＰは前記ＳＴＡと所定の暗号化アルゴリズムに基づき暗号化認証を行なうことを特徴とする。

【００２３】

また、前記暗号化認証が正常に完了した後、前記認証サーバからの指示により前記ＡＰのＭＡＣアドレスのテーブルを更新することを特徴とする。

【００２４】

さらに、前記認証サーバに障害が発生した場合に、前記ＡＰ単独にて前記ＭＡＣアドレスの認証を行なうことを特徴とする。

【００２５】

なお、前記暗号化アルゴリズムは、予め定められた使用期限を有する共通鍵に基づき暗号化されていることを特徴とする。

【００２６】

【発明の実施の形態】

本発明の無線ＬＡＮシステムの認証方法と認証装置に関する実施の形態を図面を参照して説明する。

【００２７】

（第１の実施の形態）

本発明の実施の形態の無線ＬＡＮシステムのシステム構成を示すブロック図を図1に示す。

【００２８】

本図において、ＳＴＡ(ＳＴＡＴＩＯＮ)１は、複数の端末局であり、各端末局はノートＰＣ等のデータ端末１０とデータ端末１０に挿入されて無線信号の送受信や無線信号等の制御を行うハードウェアやファームウェアとが搭載された無線ＬＡＮカード２０とから構成される。

【００２９】

ＡＰ（ＡＣＣＥＳＳ　ＰＯＩＮＴ）２は、無線アクセスと有線網とのインターフェース機能を有し、また、無線信号の送受信や無線信号等の制御を行うハードウェアやファームウェアが搭載されている。また、ＩＥＥＥ８０２．１１の認証プロトコル機能やＳＴＡ１との認証プロトコルを認証サーバの認証プロトコルに適合するようにプロトコル変換を行う機能を有する。

【００３０】

認証サーバ３は、認証機能を有するサーバであり、使用可能なＳＴＡ１のＭＡＣアドレスは事前に登録されているものとする。本実施の形態では、ダイアルアップ用アクセス、認証、課金等の機能を有するＲＡＤＩＵＳサーバを用いて説明するが、これに限るものではない。また、ＡＰ２と接続してＭＡＣアドレス認証を行う機能を有する。

【００３１】

また、保守サーバ４は、ＡＰ２をＳＮＭＰで設定、管理を行うサーバである。

【００３２】

なお、本実施の形態では認証サーバ３と保守サーバ４とを独立した構成で示しているが、同一のサーバにこれら機能を搭載することもできる。

【００３３】

ここで、ＳＴＡ１とＡＰ２との接続は無線区間５で、ＡＰ２、認証サーバ３、保守サーバ４との接続はイーサネットケーブル等の有線区間６で行われている。

【００３４】

図２は、本発明の無線ＬＡＮシステムのコントロールプレーンの各ノードにお

けるプロトコルスタックを示す図である。

【００３５】

本図において、ＩＥＥＥ８０２．１１では、帰属、認証はＭＡＣ副層の中のエンティティとして取り扱われる。無線区間５では、ＩＥＥＥ８０２．１１に基づき暗号化認証が行われる。また、ＡＰ２では、無線区間５の認証手順を受けると認証サーバ３まで認証要求を転送する。認証サーバ３は、ＲＡＤＩＵＳプロトコルを用いて認証処理を行なう。

【００３６】

図３は、本発明の無線ＬＡＮシステムの具体的な認証方法のシーケンス図である。本図は、ＩＥＥＥ８０２．１１で規定されたＷＥＰメカニズムを利用した共通鍵を用いた暗号化認証方式に加えて、ＭＡＣアドレスによる認証を行なっている。

【００３７】

前提条件として、ＳＴＡ１およびＡＰ２の鍵設定は予めされており、使用可能なＳＴＡ１のＭＡＣアドレスは認証サーバ３に登録されているものとする。

【００３８】

図１で説明したように、本発明の無線ＬＡＮシステムでは、ＳＴＡ１には無線ＬＡＮカード２０を用いているため、カードを置き忘れたり、盗難等により不正使用者の手に渡る可能性がある。このため、共通鍵に加えてＭＡＣアドレスによる認証を組み合わせて安全性を高めている。なお、本図において図６と同一手順であるものには同一の番号を用いて説明する。

【００３９】

ＳＴＡ１が立ちあがったとき、ＡＰ２に対して認証要求を送出する（Ｓ１）。このとき、ＰＤＵフォーマット内には共通鍵認証方式による認証要求であることを示すビットが用意されている。このときのＭＡＣフレーム内にはソースアドレスとしてＳＴＡ１のＭＡＣアドレスが含まれている。

【００４０】

要求を受けたＡＰ２は、図で示した通常のＷＥＰメカニズムでは、チャレンジ用のテキストを用意してＳＴＡ１へ送るが、ここではＡＰ２から認証サーバ３に

対して、ＭＡＣアドレスを認証のＩＤとして、認証サーバ３へ認証要求する（Ｓ８）。

【００４１】

ここで、認証サーバ３はＲＡＤＩＵＳサーバとして、ＩＥＴＦのＲＦＣ２１３８で定義されるＲＡＤＩＵＳ（ＲＥＭＯＴＥ　ＡＵＴＨＥＮＴＩＣＡＴＩＯＮ　ＤＩＡＬ　ＩＮ　ＵＳＥＲ　ＳＥＲＶＩＣＥ）プロトコルに基づいて動作する。

【００４２】

また、ＭＡＣアドレスは、認証用プロトコル（ＲＡＤＩＵＳプロトコル）上ではユーザー名やコーリングステイションＩＤ（ＣＡＬＬＩＮＧ－ＳＴＡＴＩＯＮ－ＩＤ）等として定義されている。

【００４３】

認証（ＲＡＤＩＵＳ）サーバ３は、ＡＰ２から受けたＭＡＣアドレスを認証する（Ｓ９）。

【００４４】

次に、ＭＡＣアドレスが認証された場合には、ＩＥＴＦのＲＦＣ１９９４で定義されるＣＨＡＰプロトコル（ＰＰＰ　ＣＨＡＬＬＥＮＧＥ　ＨＡＮＤＳＨＡＫＥ　ＡＵＴＨＥＮＴＩＣＡＴＩＯＮ　ＰＲＯＴＯＣＯＬ）と同様な手順に基づいてチャレンジテキストがＡＰ２に対して送信される（Ｓ１０）。ここで、ＰＰＰとは、Ｐｏｉｎｔ－ｔｏ－Ｐｏｉｎｔ　ＰＲＯＴＯＣＯＬをいう。

【００４５】

なお、ＣＨＡＰプロトコルでは一方向性のハッシュ方式としてメッセイジダイジェスト５（ＭＥＳＳＡＧＥ　ＤＩＧＥＳＴ　２；ＭＤ５）が定められているが、それとは異なる方式を用いたり、有線路の安全性が確保されているとする場合は、ダミープロトコルとして使用しても良い。

【００４６】

認証サーバ３からチャレンジテキストを受信したＡＰ２は本来のＷＥＰメカニズムに戻ってＳＴＡ１に対するチャレンジテキストをＳＴＡ１へ送信する（Ｓ２）。

【００４７】

なお、このチャレンジテキストは、図のチャレンジテキストと同一であっても良いし、認証サーバ３からのチャレンジテキストを流用しても良い。

【００４８】

ＳＴＡ１はＡＰ２より受信したチャレンジテキストに対し、ＷＥＰメカニズムにより自分の共通鍵とイニシャライゼイションベクタ（ＩＮＩＴＩＡＬＩＺＡＴＩＯＮ　ＶＥＣＴＯＲ；ＩＶ）により暗号化を行う（Ｓ３）。

【００４９】

この暗号文とイニシャライゼイションベクタは、ＳＴＡ１からＡＰ２へ送信される（Ｓ４）。

【００５０】

ＡＰ２は、受信した暗号文とイニシャライゼイションベクタと自分の共通鍵により暗号文を復号し、元のチャレンジテキストに戻れば、無線区間の認証が成功したものとする（Ｓ５）。

【００５１】

ＡＰ２は、認証サーバ３にＣＨＡＰによりハッシュを行ってＣＨＡＰレスポンスを返す（Ｓ１１）。

【００５２】

なお、ＣＨＡＰをダミープロトコルとする場合は、ＣＨＡＰレスポンス相当の返答に変えて返答する。

【００５３】

認証サーバ３ではＣＨＡＰにより正常なレスポンスを受け取ったことが分かると、全体の認証が完了したとして、ＡＰ２に対して認証完了の通知をする（Ｓ１２）。

【００５４】

認証完了通知を受けたＡＰ２はＳＴＡ１に対して認証完了を通知し、ＳＴＡ１も認証が成功したことを認知する（Ｓ６）。

【００５５】

また、認証サーバ３は、ＡＰ２に保存されている接続可能なＭＡＣアドレステーブルを更新するよう指示を行なう（Ｓ１３）。この結果、新たに認証されたＭ

ＡＣアドレスが随時更新登録されることになり、ＡＰ２のＭＡＣアドレス管理テーブルの動的な更新を可能とする。

【００５６】

その後、ＳＴＡ１とＡＰ２とは、アソシエーションの動作へ移る（Ｓ７）。

【００５７】

（第２の実施の形態）

本発明の第２の実施の形態は、図３のシーケンスにおいて、認証サーバ３にハードやソフト等の障害が発生し、ＡＰ２からの認証サーバ３に対する認証要求（Ｓ８）が受け付けられない場合に、ＡＰ２単体でＭＡＣアドレスによる認証を行うフローが追加されたことである。

【００５８】

これは、図３のシーケンスの（Ｓ１３）で説明したようにＡＰ２のＭＡＣアドレステーブルは動的に更新されているため、認証結果がＡＰ２のＭＡＣアドレステーブルに即時反映され、ＡＰ２は障害直前までのＭＡＣアドレス情報を知っているためＡＰ２単体のＭＡＣアドレス認証ができる。この結果、たとえ認証サーバ３に障害等が発生しても認証手順を継続することができる。

【００５９】

（第３の実施の形態）

本発明の第３の実施の形態としては、共通鍵の使用時間に予め所定の期限を設けて安全性を高めるものである。

【００６０】

図３のシーケンスの（Ｓ３）において、ＳＴＡ１の自分の共通鍵を用いて常時暗号化できるようになっていたが、共通鍵が漏洩される等の場合においても不正認証が行わることのないよう本実施形態で一定の保護を設けることができる。

【００６１】

（第４の実施の形態）

前述した本発明の第３の実施の形態では、ＷＥＰ用共通鍵に使用期限を設けることで不正使用者の保護は図れる。しかし、正規の使用者が本使用期限内にＳＴＡ１を使用しなかった場合等では、使用期限以降に再度使用可能とするため鍵の

配送を行う必要がある。

【００６２】

本発明の第４の実施の形態はこのような共通鍵が使用期限により無効となった場合の認証方法に関するものである。

【００６３】

図４は、本発明の第４の実施の形態の認証手順を示すシーケンス図を示している。

【００６４】

本図において、ＳＴＡ１からの共通鍵認証が無効となった場合、ＳＴＡ１はＡＰ２に対して再度オープンシステム認証方式により認証要求する（Ｓ１４）。

【００６５】

要求されたＡＰ２は、オープンシステム認証方式であることを知り、ＡＰ１から認証サーバ３に対して、ＭＡＣアドレスを認証のＩＤとして認証要求する（Ｓ１５）。

【００６６】

ここで、認証サーバ３は、例えば、ＲＡＤＩＵＳサーバとしてＩＥＴＦのＲＦＣ２１３８で定義されるＲＡＤＩＵＳプロトコルに基づいて動作する。

【００６７】

また、ＭＡＣアドレスは、認証用プロトコル（ＲＡＤＩＵＳ）上ではユーザー名やコーリングステイションＩＤ（ＣＡＬＬＩＮＧ－ＳＴＡＴＩＯＮ－ＩＤ）等として定義されている。

【００６８】

次に、認証（ＲＡＤＩＵＳ）サーバ３は、ＭＡＣアドレスを認証した後、ＩＥＴＦのＲＦＣ１９９４で定義されるＣＨＡＰプロトコルと同様な手順に基づいてチャレンジテキストがＡＰ２に対して送信される（Ｓ１６）。

【００６９】

ここで、ＣＨＡＰプロトコルでは一方向性のハッシュ方式としてＭＤ５が定められているが、それとは異なる方式を用いたり、有線路の安全性が確保されているとする場合は、ダミープロトコルとして使用しても良い。

【００７０】

認証サーバ３からチャレンジテキストを受信したＡＰ２は認証サーバ３に対しＣＨＡＰによりハッシュを行ってＣＨＡＰレスポンスを返す（Ｓ１７）。

【００７１】

なお、ＣＨＡＰをダミープロトコルとする場合は、ＣＨＡＰレスポンス相当の返答に変えて返答する。

【００７２】

認証サーバ３は、ＣＨＡＰにより正常なレスポンスを受け取ったことが分かると、全体の認証が完了したとして、ＡＰ２に対して認証完了の通知をする（Ｓ１８）。

【００７３】

認証完了通知を受けたＡＰ２はＳＴＡ１に対して認証完了通知し、ＳＴＡ１も認証が成功したことを認知する（Ｓ１９）。

【００７４】

その後、ＳＴＡ１とＡＰ２とはアソシエーションの動作へ移る（Ｓ２０）。

【００７５】

なお、ＡＰ２と認証サーバ３間で認証に成功した場合、第１の実施の形態で説明したようにＡＰ２に保存されている接続可能ＭＡＣアドレステーブルに対して、新たに認証したＭＡＣアドレスを更新登録しても良いが、本実施の形態の場合にはオープンシステム認証方式なので安全性が低いためＭＡＣアドレスの更新登録を行わないのが望ましい。

【００７６】

アソシエーション手順が完了すれば、ＳＴＡ１はＡＰ２を通して通常のＩＰパケットによる通信を行なう（Ｓ２１）。

【００７７】

（第５の実施の形態）

第４の実施の形態におけるオープンシステム認証方式の場合に、アソシエーション後の通信期間に制限がなかったため、不正接続が行われる可能性が高い。

【００７８】

本発明の第５の実施の形態では、アソシエーション後の通信期間の有効期間を、例えば、公開鍵配送方式などにより鍵管理サーバからＷＥＰメカニズムの共通鍵を配送されるに十分な一定の短い時間に定める。この時間は、例えば、１０秒から１分程度が望ましい。

【００７９】

そして、図４において、本来の共通鍵認証のための鍵配送を受けた後、デアソシエーションし（Ｓ２２）、再度共通鍵認証方式で接続する。

この結果、ＭＡＣアドレスを偽る不正アクセスがあったとしても、セキュリティを向上する効果をもたらす。

【００８０】

【発明の効果】

以上説明したように、本願発明の無線ＬＡＮシステムの認証方法および認証装置は、以下の効果を有している。

【００８１】

第１に、ＩＥＥＥ８０２．１１で規定された共通鍵認証方式を拡張してＭＡＣアドレス認証を行なっている。このため、無線ＬＡＮカードを用いるため不正使用等が起きやすい無線ＬＡＮシステムにおいても、高い安全性を確保することができる。また、非常に多数の無線ＬＡＮカードに対する認証をいずれのアクセスポイントからでも行なえる効果も有している。

【００８２】

第２に、ＷＥＰの共通鍵に使用期限を設けたり、オープンシステム認証方式でアソシエーションされている期間を限定したりしてさらに、安全性を高めることができる。

【００８３】

第３に、ＡＰにおけるＭＡＣアドレステーブルは認証サーバからの指示で動的に更新されているため、認証サーバが障害になっても、障害直前までのＭＡＣアドレス情報を利用してＡＰ単独でＭＡＣアドレス認証ができる。

なお、本発明が上記各実施の形態に限定されず、本発明の技術思想の範囲内において、各実施の形態は適宜変更され得ることは明らかである。

【図面の簡単な説明】

【図１】

本発明の無線ＬＡＮシステムのシステム構成を示すブロック図である。

【図２】

図１の各ノードのプロトコルスタックを示す図である。

【図３】

図１の認証手順を示すシーケンス図である。

【図４】

本発明の共通鍵が無効になった場合の認証手順を示すシーケンス図である。

【図５】

ＩＥＥＥ８０２．１１に規定された無線ＬＡＮシステムの認証方法に関するシステム構成を示すブロック図である。

【図６】

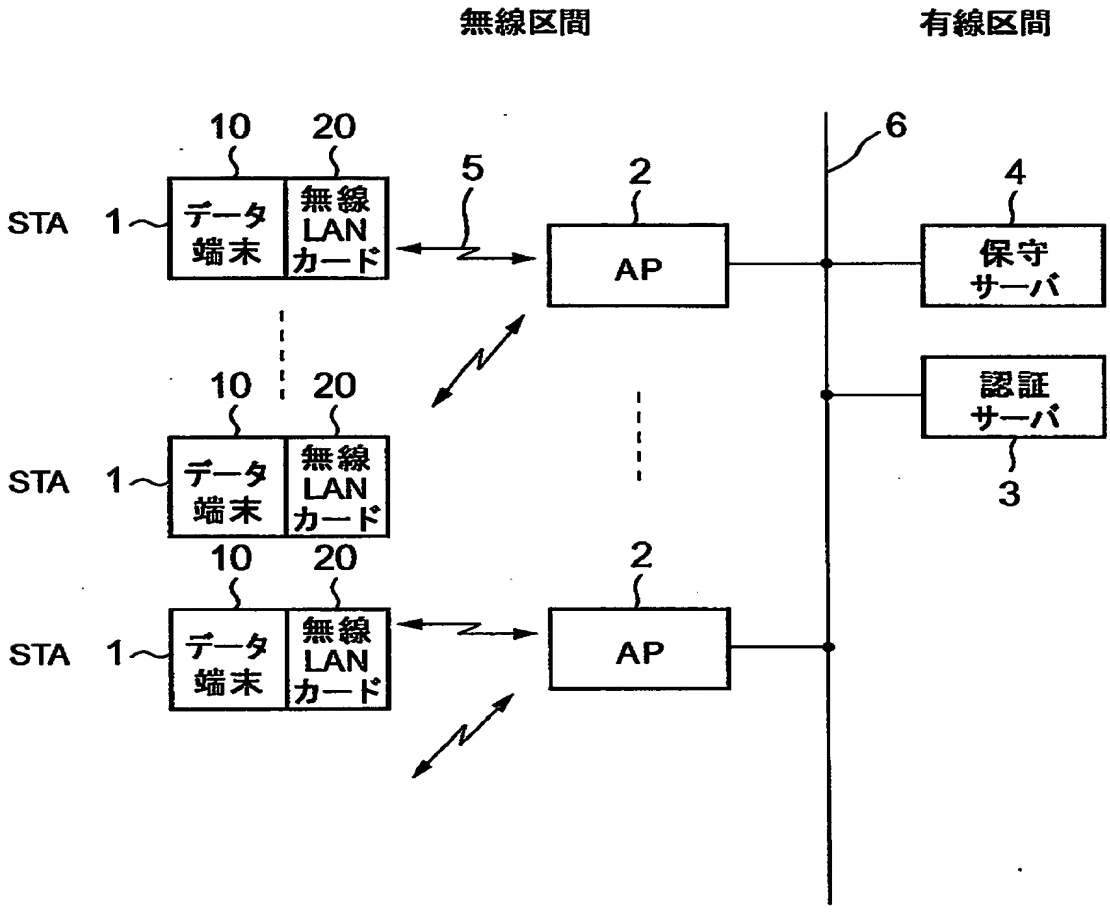
図５の認証手順を示すブロック図である。

【符号の説明】

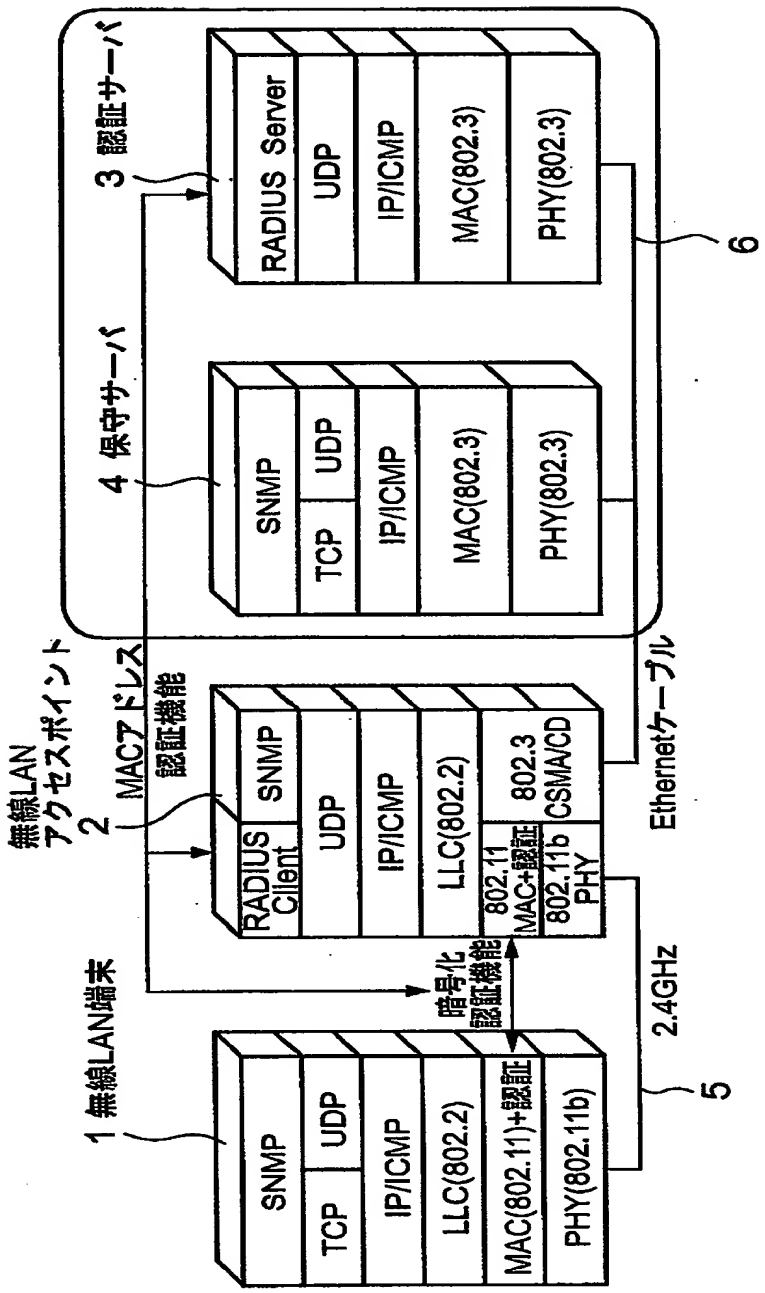
１	ＳＴＡ
２	ＡＰ
３	認証サーバ
４	保守管理サーバ
５	無線区間
６	有線区間
１０	ノートＰＣ等
２０	無線ＬＡＮカード

【書類名】　図面

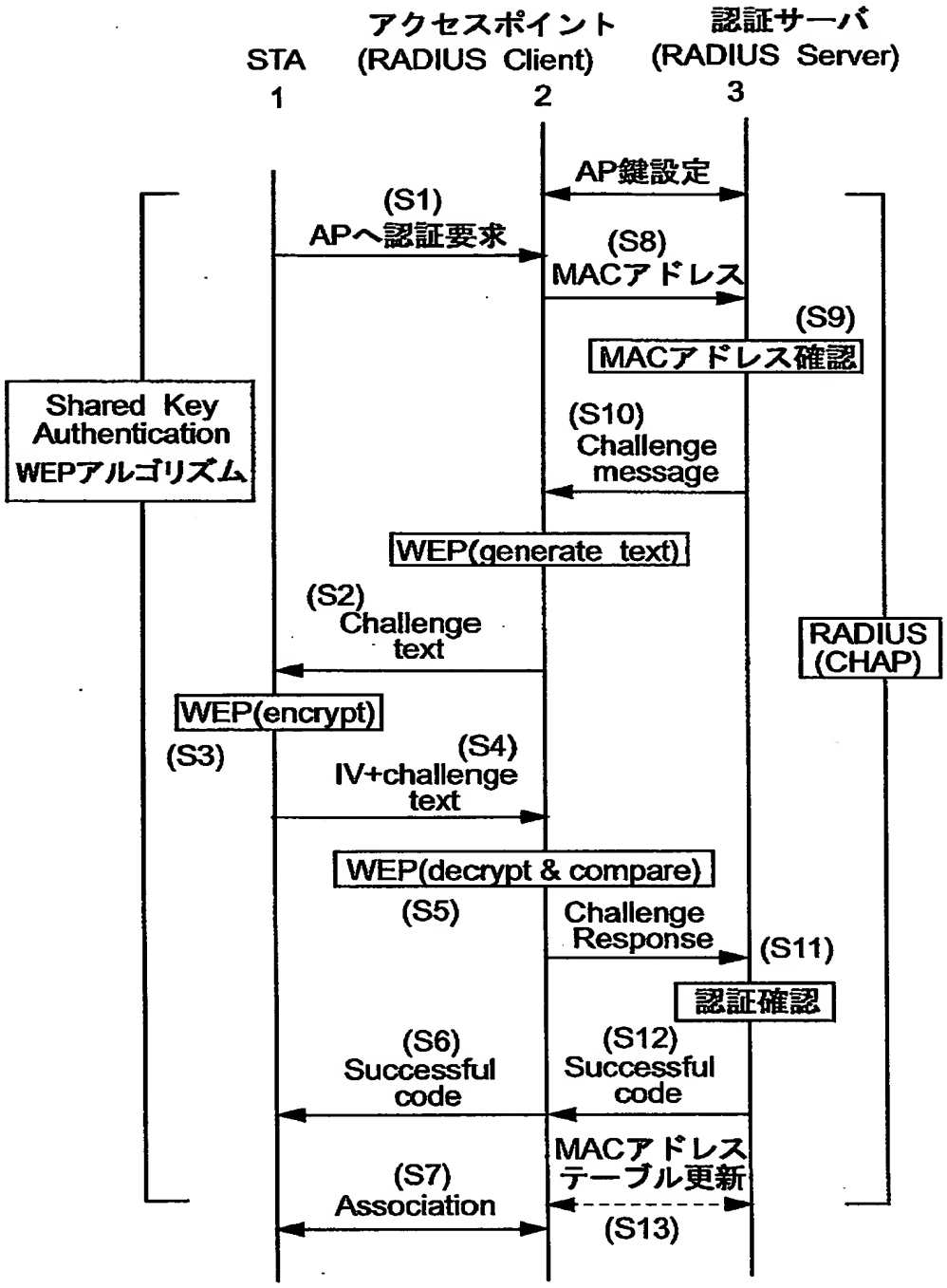
【図１】



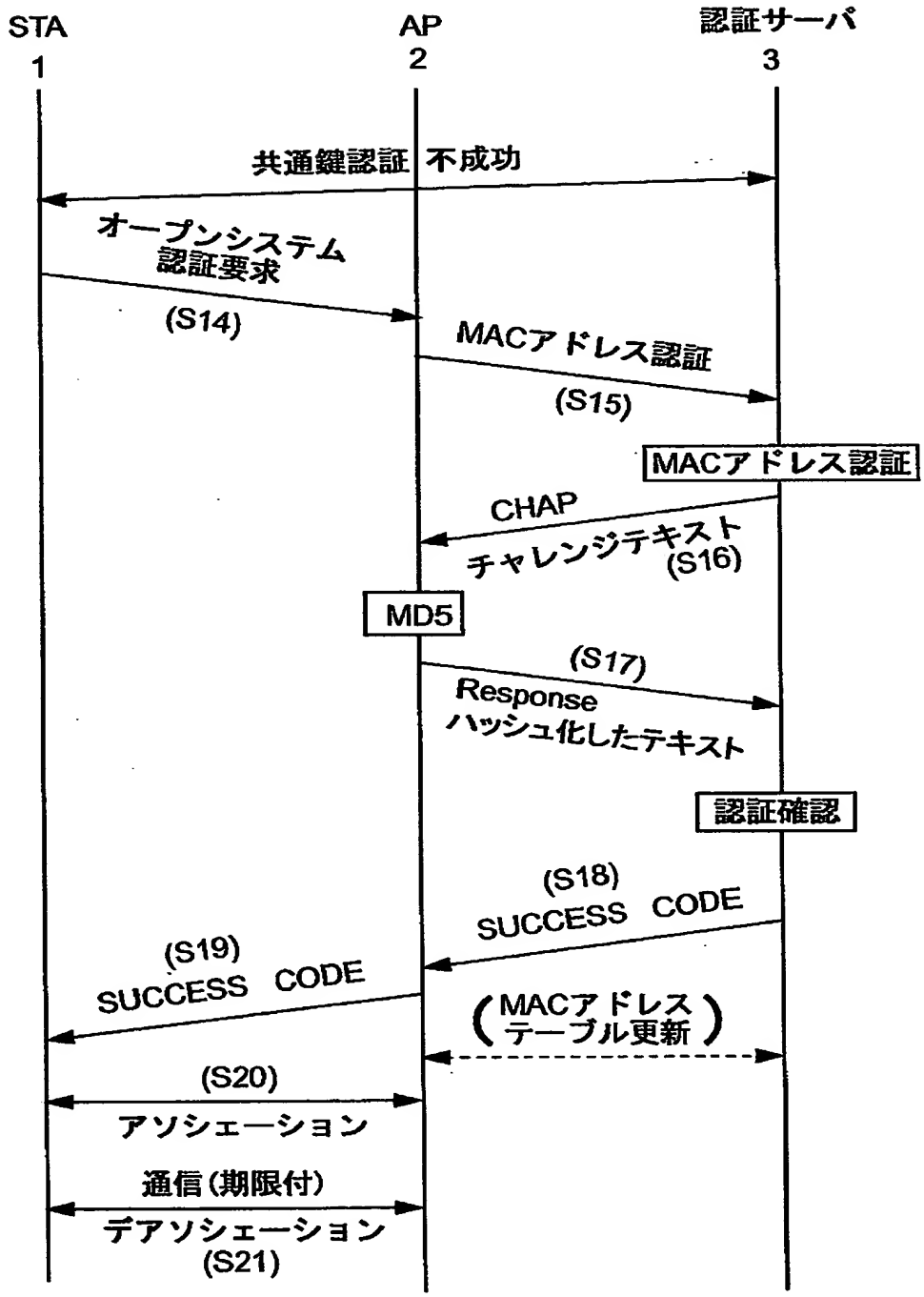
【図２】


3 認証サーバ
RADIUS Server
UDP
IP/ICMP
MAC(802.3)
PHY(802.3)
4 保守サーバ
SNMP
TCP
UDP
IP/ICMP
MAC(802.3)
PHY(802.3)
6
無線LAN
アクセスポイント
2
MACアドレス
認証機能
RADIUS Client
SNMP
UDP
IP/ICMP
LLC(802.2)
802.11 MAC+認証
802.11b PHY
802.3 CSMA/CD
Ethernetケーブル
暗号化
認証機能
2.4GHz
5
1 無線LAN端末
SNMP
TCP
UDP
IP/ICMP
LLC(802.2)
MAC(802.11)+認証
PHY(802.11b)

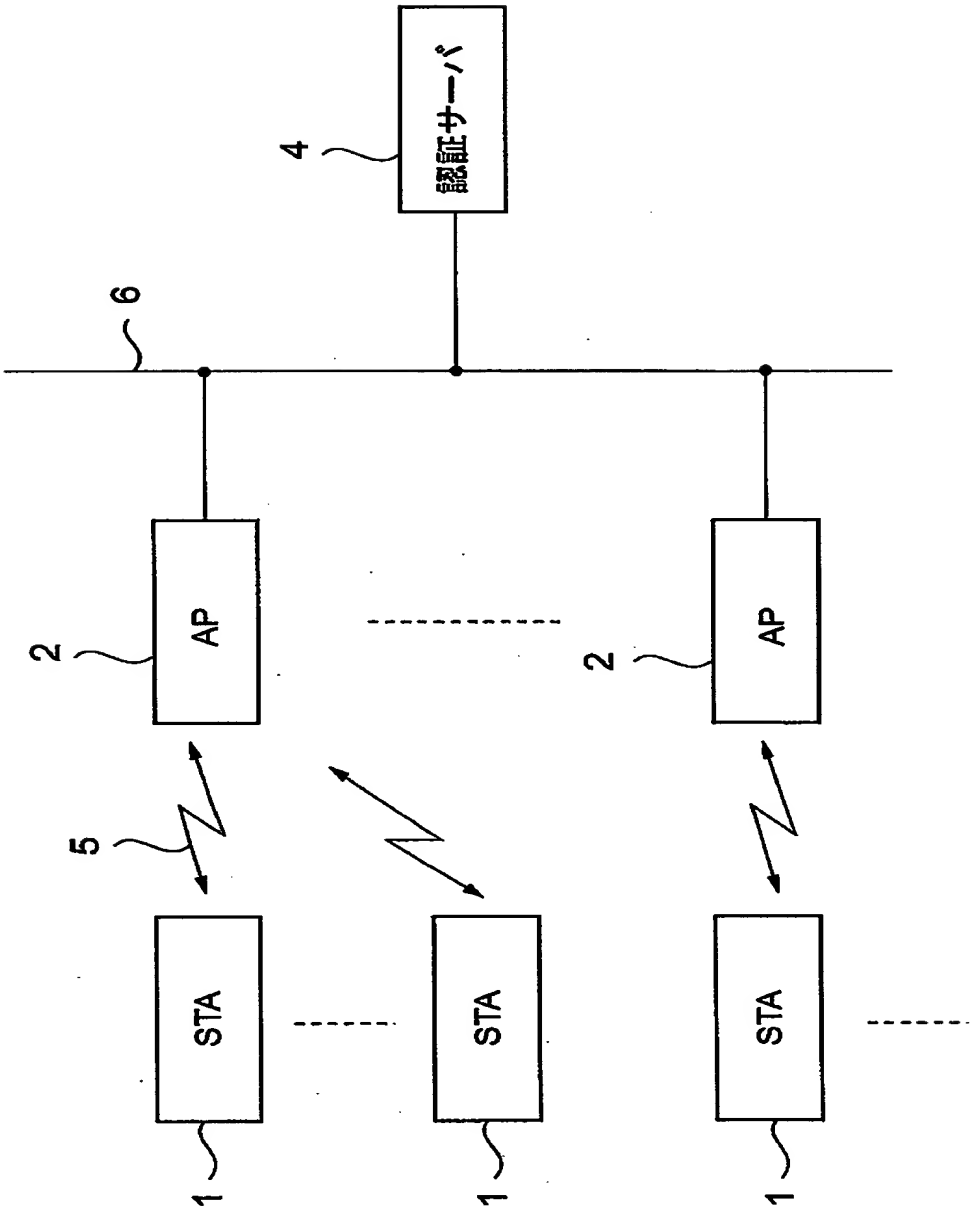
【図３】


STA
1
アクセスポイント
(RADIUS Client)
2
認証サーバ
(RADIUS Server)
3
AP鍵設定
(S1)
APへ認証要求
(S8)
MACアドレス
(S9)
MACアドレス確認
Shared Key
Authentication
WEPアルゴリズム
(S10)
Challenge
message
WEP(generate text)
(S2)
Challenge
text
RADIUS
(CHAP)
WEP(encrypt)
(S3)
(S4)
IV+challenge
text
WEP(decrypt & compare)
(S5)
Challenge
Response
(S11)
認証確認
(S6)
Successful
code
(S12)
Successful
code
MACアドレス
テーブル更新
(S7)
Association
(S13)

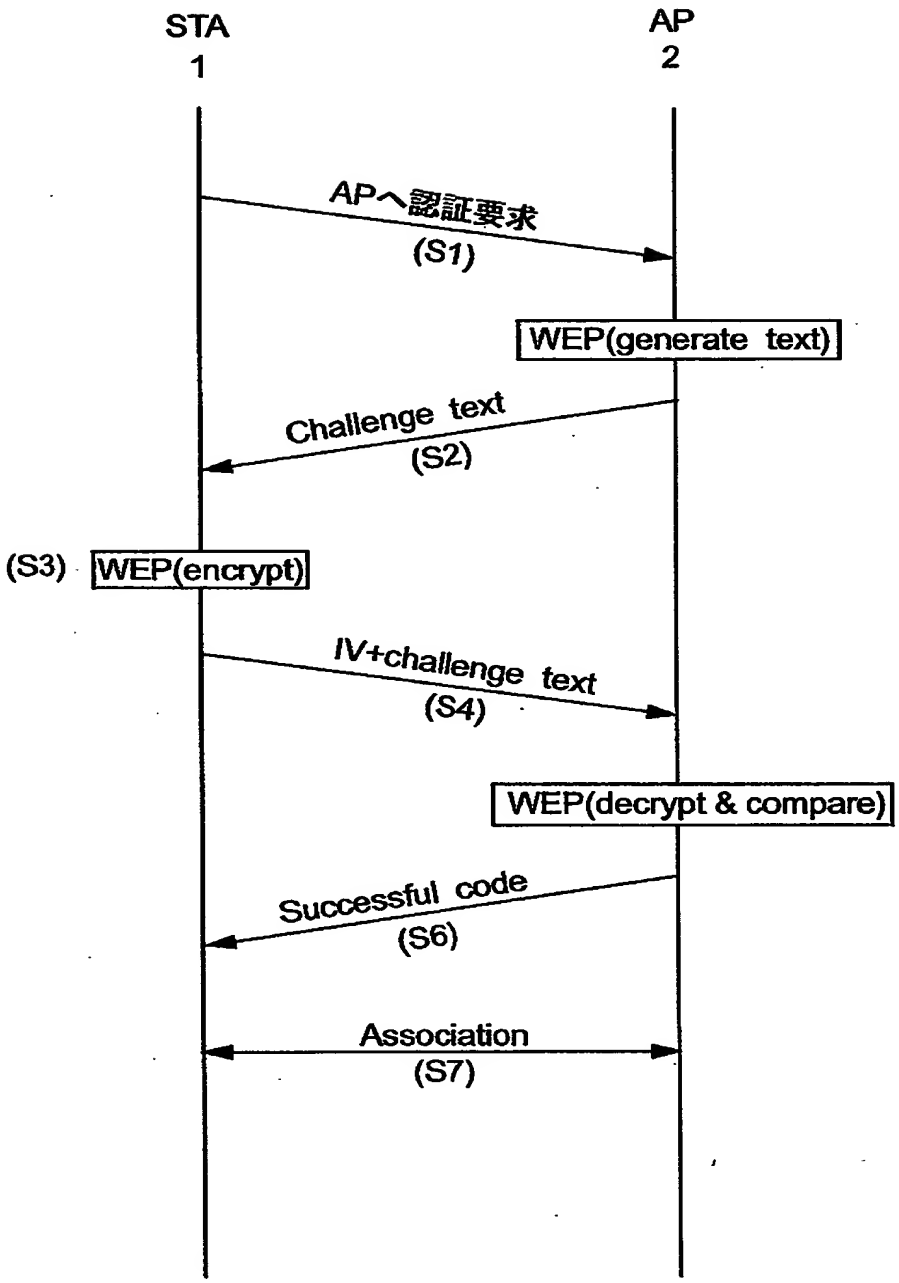
【図４】


STA
1
AP
2
認証サーバ
3
共通鍵認証 不成功
オープンシステム
認証要求
(S14)
MACアドレス認証
(S15)
MACアドレス認証
CHAP
チャレンジテキスト
(S16)
MD5
(S17)
Response
ハッシュ化したテキスト
認証確認
(S18)
SUCCESS CODE
(S19)
SUCCESS CODE
(MACアドレス
テーブル更新)
(S20)
アソシエーション
通信(期限付)
デアソシエーション
(S21)

【図５】



【図６】


STA
1
AP
2
APへ認証要求
(S1)
WEP(generate text)
Challenge text
(S2)
(S3)
WEP(encrypt)
IV+challenge text
(S4)
WEP(decrypt & compare)
Successful code
(S6)
Association
(S7)

【書類名】　要約書

【要約】

【課題】ＩＥＥＥ８０２．１１に準拠した無線ＬＡＮシステムの暗号化認証方法と認証装置について、アクセスポイント（ＡＰ）に多数の加入者局（ＳＴＡ）を接続して安全に認証できる構成を提供する。

【解決手段】データ端末１０と無線ＬＡＮカード２０からなる多数のＳＴＡ１からＡＰ２に対して認証要求を送出する（Ｓ１）。ＡＰ２は認証サーバ（ＲＡＤＩＵＳ）サーバ３に対して、認証サーバ３のプロトコルでＭＡＣアドレスを送出する（Ｓ８）。認証サーバ３は、ＭＡＣアドレス認証を実行した（Ｓ９）後、チャレンジテキストをＡＰ２に送出する（Ｓ１０）。ＡＰ２は、１ＥＥＥ８０２．１１で定められたＷＥＰアルゴリズムの処理に従って、ＳＴＡ１と暗号化認証を行なう（Ｓ２）～（Ｓ６）。

【選択図】図３

認定・付加情報

特許出願の番号	平成１１年　特許願　第２８４２３１号
受付番号	５９９００９７５０３７
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１１年１０月　７日

＜認定情報・付加情報＞

【提出日】　平成11年10月 5日

次頁無

出証特２０００－３０５４４５６

出　願　人　履　歴　情　報

識別番号　　〔０００００４２３７〕

１．変更年月日　　１９９０年　８月２９日
［変更理由］　新規登録
住　所　東京都港区芝五丁目７番１号
氏　名　日本電気株式会社